(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
2 June 2005 (02.06.2005)

PCT

(10) International Publication Number
WO 2005/050423 A1

(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number:
PCT/US2004/036832

(22) International Filing Date:
5 November 2004 (05.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/715,970 17 November 2003 (17.11.2003) US

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **BAJIKAR, Sundeep** [IN/US]; 930 Cole Place, Santa Clara, CA 95054 (US).

(74) Agent: **VINCENT, Lester, J.**; Blakely, Sokoloff, Taylor & Zafman, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, CA 90025 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 2005/050423 A1

(54) Title: METHOD AND SYSTEM TO PROVIDE A TRUSTED CHANNEL WITHIN A COMPUTER SYSTEM FOR A SIM DEVICE

(57) Abstract: Exchanging data between a SIM device (180) and an application executed in a trusted platform (110,120,140), wherein the data to be exchanged is secured from unauthorized access. In one embodiment, the exchanging data includes exchanging an encryption key via a trusted path within a computer system(100), and exchanging data encrypted with the encryption key, via an untrusted path with the computer system.

Method and System To Provide A Trusted Channel Within A Computer System For A SIM Device

Field of Invention

[0001] The field of invention relates generally to trusted computer platforms; and, more specifically, to a method and apparatus to provide a trusted channel within a computer system for a SIM device.

Background

[0002] Trusted operating systems (OS) and platforms are a relatively new concept. In first generation platforms, a trusted environment is created where applications can run trustedly and tamper-free. The security is created through changes in the processor, chipset, and software to create an environment that cannot be seen by other applications (memory regions are protected) and cannot be tampered with (code execution flow cannot be altered). As a result, the computer system cannot be illegally accessed by anyone or compromised by viruses.

[0003] In today's computing age, Subscripber Identify Modules (SIM), sometimes referred to as a smart card, are becoming more prevalent. A SIM is a credit card sized card that is typically used for Global System for Mobile communications (GSM) phones to store telephone account information and provide Authentication, Authorization and Accounting (AAA). The SIM cards also allow a user to use a borrowed or rented GSM phone as if it were their own. SIM cards can also be programmed to display custom menus on the phone's readout. In some cases, the SIM cards include a built-in microprocessor and memory that may be used in some cases for identification or financial transactions. When inserted into a reader, the SIM is accessible to transfer data to and from the SIM. SIM cards may also be inserted into

[0004] When using a SIM card in a computer system, there is a need to securely access information from the SIM card in order to prevent accesses to the SIM from unauthorized software applications. Such accesses may be intended to learn certain SIM secrets or to break GSM authentication mechanisms and steal services provided

Figures

[0005] One or more embodiments are illustrated by way of example, and not limitation, in the Figures of the accompanying drawings, in which

[0006] **Figure 1** illustrates a computer system capable of providing a trusted platform to protect selected applications and data from unauthorized access, according to one embodiment; and

[0007] **Figure 2** is a flow diagram describing a process of providing a trusted channel within a computer system for a SIM device, according to one embodiment.

Detailed Description

[0008] A method and system to provide a trusted channel within a computer system for a SIM device is described. In one embodiment, data is exchanged between an application being executed in a trusted platform and a SIM device, wherein the data exchanged is protected from unauthorized access. In one embodiment, an encryption key is exchanged via a trusted channel within a computer system. Data encrypted with the encryption key is exchanged via an untrusted channel within the computer system.

[0009]In the following description, numerous specific details are set forth. However, it is understood that embodiments may be practiced without these specific details. In other instances, well-known circuits, structures and techniques have not been shown in detail in order not to obscure the understanding of this description.

[0010]Reference throughout this specification to "one embodiment" or "an embodiment" indicate that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment. Thus, the appearances of the phrases "in one embodiment" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more embodiments. In addition, as described herein, a trusted platform, components, units, or subunits thereof, are interchangeably referenced as a protected or secured.

Trusted Platform

[0011] Fig. 1 illustrates a computer system, according to one embodiment, capable of providing a trusted platform to protect selected applications and data from unauthorized access. System 100 of the illustrated embodiment includes a processors 110, a chipset 120 connected to processors 110 via processor bus 130, a memory 140, and a SIM device 180 to access data on a SIM card 182. In alternative embodiments, additional processors and units may be included.

[0012] Processor 110 may have various elements, which may include but are not limited to, embedded key 116, page table (PT) registers 114 and cache memory (cache) 112. All or part of cache 112 may include, or be convertible to, private memory (PM) 160. Private memory is a memory with sufficient protections to prevent access to it by any unauthorized device (e.g., any device other than the associated processor 110) while activated as a private memory.

[0013] Key 116 may be an embedded key to be used for encryption, decryption, and/or validation of various blocks of data and/or code. Alternatively, the key 116 may be provided on an alternative unit within system 100. PT registers 114 may be a table in the form of registers to identify which memory pages are to be accessible only by trusted code and which memory pages are not to be so protected.

[0014] In one embodiment, the memory 140 may include system memory for system 100, and in one embodiment may be implemented as volatile memory commonly referred to as random access memory (RAM). In one embodiment, the memory 140 may contain a protected memory table 142, which defines which memory blocks (where a memory block is a range of contiguously addressable memory locations) in memory 140 are to be inaccessible to direct memory access

(DMA) transfers. Since all accesses to memory 140 go through chipset 120, chipset 120 may check protected memory table 142 before permitting any DMA transfer to take place. In a particular operation, the memory blocks protected from DMA transfers by protected memory table 142 may be the same memory blocks restricted to protected processing by PT registers 144 in processor 110. The protected memory table 142 may alternatively be stored in a memory device of an alternative unit within system 100.

[0015] In one embodiment, Memory 140 also includes trusted software (S/W) monitor 144, which may monitor and control the overall trusted operating environment once the trusted operating environment has been established. In one embodiment, the trusted S/W monitor 144 may be located in memory blocks that are protected from DMA transfers by the protected memory table 142.

[0016] Chipset 120 may be a logic circuit to provide an interface between processors 110, memory 140, SIM device 180, and other devices not shown. In one embodiment, chipset 120 is implemented as one or more individual integrated circuits, but in other embodiments, chipset 120 may be implemented as a portion of a larger integrated circuit. Chipset 120 may include memory controller 122 to control accesses to memory 140. In addition, in one embodiment, the chipset 120 may have a SIM reader of the SIM device integrated on the chipset 120.

[0017] In one embodiment, protected registers 126 are writable only by commands that may only be initiated by trusted microcode in processors 110. Trusted microcode is microcode whose execution may only be initiated by authorized instruction(s) and/or by hardware that is not controllable by unauthorized devices. In one embodiment, trusted registers 126 hold data that identifies the locations of, and/or controls access to, trusted memory table 142 and trusted S/W monitor 144. In one embodiment, trusted registers 126 include a register to enable or disable the use of trusted memory table 142 so that the DMA protections may be activated before entering a trusted operating environment and deactivated after leaving the trusted operating environment.

Trusted Channel with SIM Device

[0018] **Fig. 2** is a flow diagram describing a process of providing a trusted channel within a computer system for a SIM device, according to one embodiment. As described herein, reference to a SIM device includes other types of related Smart cards. The processes described in the flow diagram of **Fig. 2**, are described with reference to the system of **Fig. 1**, described above.

[0019]In one embodiment, in process 202, an application 150 being executed in a trusted environment of the system 100, determines information is to be accessed from a SIM device 180 of the system 100. The application 150 being executed in a trusted atmosphere can be located in a protected memory, such as protected memory 160 of cache 112, or a protected section of memory 140. In one embodiment, the SIM device 180 includes a mechanism to ascertain that the accesses are coming from the application in a trusted environment that is running on the same platform that the SIM device is physically attached to, and not from some remotely executing application.

[0020] In process 204, the application and the SIM device perform a mutual authentication to determine that the SIM device is the correct device from which the application is to receive data, or that the application is the correct application to which the SIM device is to send the data. The mutual authentication may be conducted via a variety of processes known throughout the concerned field of technology.

[0021] In process 206, following the completion of the mutual authentication, in one embodiment, the application 150 transmits an encryption key to a protected section of memory 140, via a trusted channel with the memory device, and corresponding PT entries held in the CPU. In one embodiment, the protected section of memory to store the encryption key is identifiable via the protected memory table 142.

[0022] The encryption key provided by the application 150 to the protected section of memory 140, is generated by the application 150, and is applicable to one of several available encryption processes, such as the Data Encryption Standard (DAS) or the Advanced Encryption Standard (AES). In one embodiment, the encryption key is generated via utilization of the key 116 of processor 110.

[0023] In process 208, the SIM device 180 accesses the encryption key from the protected section of memory 140. In one embodiment, the SIM device accesses the encryption key via a trusted port 112, of a chipset 120, which is mapped to the protected section of memory 140. In one embodiment, the trusted port may support one several platform bus protocols, including USB. In an alternative embodiment, the encryption key is provided by the SIM device, wherein the application accesses the encryption key from the SIM device via the trusted port of the chipset.

[0024] In process 210, the SIM device 180 uses the encryption key to encrypt data to be sent to the application 150. In process 212, the encrypted packets are transferred from the SIM device 180 by a host controller 128 (e.g., a USB host controller) of the chipset to a regular area of memory (i.e., unprotected section of memory 148). For example, an area of memory that is used to store data packets, such as USB data packets.

[0025] In one embodiment, the encrypted packets are transmitted to the memory by the host controller via a regular port 120 of the chipset (i.e., an unprotected port), which maps to an unprotected section of memory 148. In one embodiment, the encrypted packets from the SIM device include Message Authentication Code (MAC) to provide a level of integrity protection.

[0026] In process 214, a driver (e.g., an unprotected USB driver) accesses the encrypted packets from the unprotected section of memory 148 and provides the encrypted packets to the application 150 being executed in the trusted environment. In process 216, the application 150 decrypts the encrypted packets to access the data from the SIM device, which have been securely transferred to the application via an untrusted path within the system 100.

[0027] In one embodiment, new encryption keys may be exchanged based on predetermined events. For example, a new encryption key may be exchanged following one of, or a combination of, each new transaction (as defined based on implementation choice), the passage of a predetermined period of time, or the exchange of a predetermined amount of data.

[0028] In another alternative embodiment, multiple encryption keys are exchanged between the application 150 and the SIM device 180, to be used encrypted data exchanges between the SIM device 180 and the application 150. For example, a SIM device may include multiple data pipes (e.g., bulk-in, bulk-out, and default control pipes). For each of the data pipes of the SIM device, a separate encryption key may be used to protect the data exchanges. Alternatively, the separate data pipes may all use the same encryption key.

[0029] In an alternative embodiment, the data packets may be transmitted from the SIM device to the application without the use of encryption. For example, the host controller 128 transmits the data from the SIM device to the protected section of memory 140 via the trusted port 112 of the chipset 120. A trusted driver would then access the data from the protected section of memory 140 and provide the data to the application 150 via a trusted path, without having the SIM data encrypted.

[0030]The processes described above can be stored in the memory of a computer system as a set of instructions to be executed. In addition, the instructions to perform the processes described above could alternatively be stored on other forms of machine-readable media, including magnetic and optical disks. For example, the processes described could be stored on machine-readable media, such as magnetic disks or optical disks, which are accessible via a disk drive (or computer-readable medium drive). Further, the instructions can be downloaded into a computing device over a data network in a form of compiled and linked version.

[0031]Alternatively, the logic to perform the processes as discussed above could be implemented in additional computer and/or machine readable media, such as discrete hardware components as large-scale integrated circuits (LSI's), application-specific integrated circuits (ASIC's), firmware such as electrically erasable programmable read-only memory (EEPROM's); and electrical, optical, acoustical and other forms of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.); etc.

[0032] In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention as set forth in the appended claims. In particular, as described herein, the SIM device is inclusive of Smart card devices, including USB Chip/Smart Card Interface Devices (CCID). Furthermore, the architecture of the system as described herein is independent of any particular key exchange protocols that are used. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

Claims

1) A method comprising:

exchanging data between a SIM device and an application executed in a trusted platform, wherein the data to be exchanged is secured from unauthorized access.

2) The method of claim 1, wherein the exchanging of data include:

exchanging an encryption key via a trusted path within a computer system; and

exchanging data encrypted with the encryption key, via an untrusted path within the computer system.

3) The method of claim 2, wherein the exchanging the encryption key includes the application transmitting the encryption key to a protected section of memory within the computer system; and

a SIM device accessing the encryption key from the protected section of memory.

4) The method of claim 2, wherein the exchanging the encryption key includes the application accessing the encryption key from the SIM device, the application accessing the encryption key via a trusted port of a chipset.

5) The method of claim 2, wherein the exchanging the encryption key includes exchanging multiple encryption keys, and the exchanging data includes exchanging separate units of data, with each unit of data separately encrypted with an encryption key selected from the multiple encryption keys.

6) The method of claim 2, wherein the exchanging data includes a host controller transmitting data from the SIM device to an unprotected section of memory.

7) The method of claim 6, wherein the exchanging data includes a driver transmitting data from the unprotected section of memory to the application.

8) The method of claim 7, wherein the host controller is a Universal Serial Bus (USB) host controller and the driver is a USB driver.

9) The method of claim 6, wherein the exchanging the encryption key includes the SIM device reading the encryption key from the protected section of memory via a trusted port of a chip set.

10) The method of claim 6 further including:

the application decrypting the encrypted data using the encryption key.

11) The method of claim 7 further including

prior to exchanging the encryption key, the application authenticating the SIM device.

12) The method of claim 6, further including:

exchanging a new encryption key based on a predetermined event selected from a group comprising of, each new transaction, passage of a predetermined period of time, and exchange of a predetermined amount of data.

13) A system comprising:

a processor;

a memory having a protected section and an unprotected section;

a SIM device; and

a chipset to Exchange data between the SIM device and an application executed in a trusted platform, wherein the data to be exchanged is secured from unauthorized access.

14) The system of claim 13, wherein the exchange of data is to include an exchange of an encryption key via a trusted path within a computer system, and an exchange of data encrypted with the encryption key, via an untrusted path within the computer system.

15) The system of claim 14, wherein the exchange of the encryption key includes the application to transmit the encryption key to the protected section of memory, and the SIM device to access the encryption key from the protected section of memory.

16) The system of claim 13, wherein the exchange of the encryption key includes the application to access the encryption key from the SIM device, the application to access the encryption key via a trusted port of a chipset.

17) The system of claim 13, wherein the exchange of the encryption key includes an exchange of multiple encryption keys, and the exchange of data includes an exchange of separate units of data, with each unit of data separately encrypted with an encryption key selected from the multiple encryption keys.

18) The system of claim 12, wherein the system further includes a host controller to transmit data from the SIM device to an unprotected section of memory.

19) The system of claim 16, wherein the system further includes a driver to transmit data from the unprotected section of memory to the application.

20) The system of claim 17, wherein the host controller is a Universal Serial Bus (USB) host controller and the driver is a USB driver.

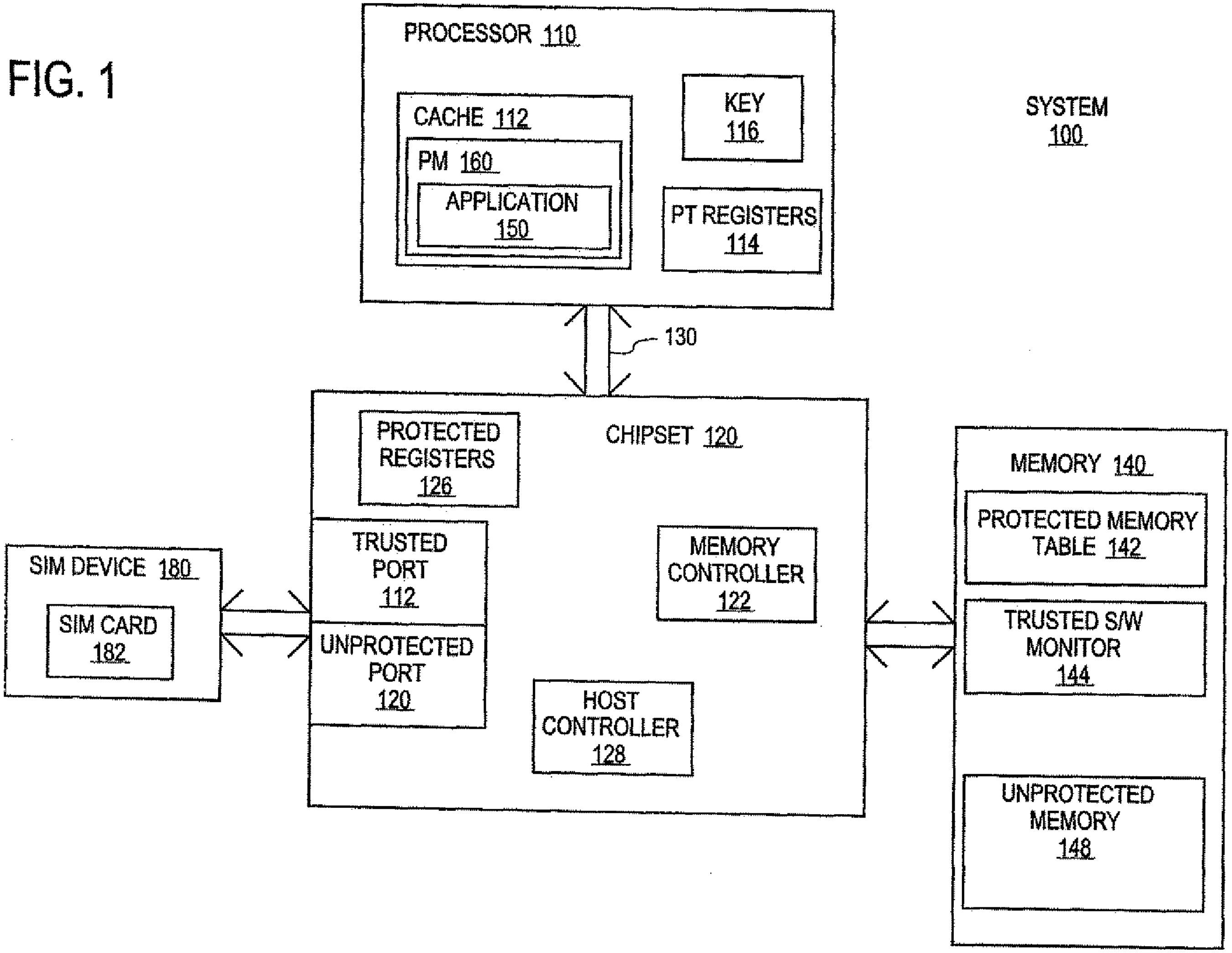
21) The system of claim 14, wherein the SIM device is to read the encryption key from the protected section of memory via a trusted port of the chip set.

22) The system of claim 14, wherein the application is to decrypt the encrypted data using the encryption key.

23) The system of claim 17, wherein the application is to authenticate the SIM device prior to the exchange of the encryption key.

24) The system of claim 14, wherein a new encryption key is to be exchanged based on a predetermined event selected from a group comprising of, each new transaction, passage of a predetermined period of time, and exchange of a predetermined amount of data.

FIG. 1


SYSTEM 100
PROCESSOR 110
CACHE 112
PM 160
APPLICATION 150
KEY 116
PT REGISTERS 114
130
CHIPSET 120
PROTECTED REGISTERS 126
TRUSTED PORT 112
UNPROTECTED PORT 120
MEMORY CONTROLLER 122
HOST CONTROLLER 128
SIM DEVICE 180
SIM CARD 182
MEMORY 140
PROTECTED MEMORY TABLE 142
TRUSTED S/W MONITOR 144
UNPROTECTED MEMORY 148

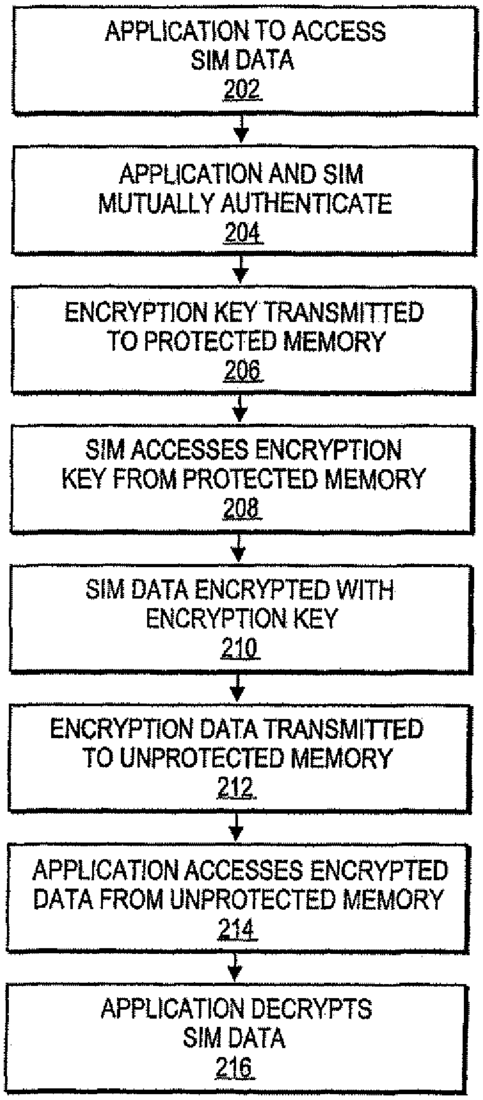

APPLICATION TO ACCESS SIM DATA
202
APPLICATION AND SIM MUTUALLY AUTHENTICATE
204
ENCRYPTION KEY TRANSMITTED TO PROTECTED MEMORY
206
SIM ACCESSES ENCRYPTION KEY FROM PROTECTED MEMORY
208
SIM DATA ENCRYPTED WITH ENCRYPTION KEY
210
ENCRYPTION DATA TRANSMITTED TO UNPROTECTED MEMORY
212
APPLICATION ACCESSES ENCRYPTED DATA FROM UNPROTECTED MEMORY
214
APPLICATION DECRYPTS SIM DATA
216

FIG. 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/036832

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/13198 A (HEWLETT-PACKARD COMPANY; PEARSON, SIANI, LYNNE; PROUDLER, GRAEME, JOHN) 22 February 2001 (2001-02-22) page 1, line 1 - page 23, line 19; figures 3,6-8 page 27, line 23 - page 30, line 21; figures 16,17,19	1-24
A	"Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1b" TCPA MAIN SPECIFICATION, XX, XX, 22 February 2002 (2002-02-22), page COMPLETE332, XP002294897 paragraph '001.! - paragraph '3.5.!	1-24

-/--

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 15 February 2005	Date of mailing of the international search report 01/03/2005
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Günther, S

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003/018892 A1 (TELLO JOSE) 23 January 2003 (2003-01-23) paragraph '0004! - paragraph '0053!; figures 1,2,6 paragraph '0353! - paragraph '0398!; figure 17	1-24
A	US 6 233 683 B1 (CHAN ALFRED ET AL) 15 May 2001 (2001-05-15) column 1, line 20 - column 4, line 38; figures 1-3b	1-24
A	DREWS S: "Standardisierung USB für Smart Cards" INTERNET CITATION, 'Online! 4 February 2003 (2003-02-04), pages I-9, XP002317401 Retrieved from the Internet: URL:http://www.sit.fraunhofer.de/german/SICA/sica_projects/smartcard-ws/> 'retrieved on 2005-02-11! the whole document	1-24

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2004/036832

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0113198 A	22-02-2001	EP 1076279 A1	14-02-2001
		DE 60002893 D1	26-06-2003
		DE 60002893 T2	13-05-2004
		EP 1203278 A1	08-05-2002
		EP 1204910 A1	15-05-2002
		WO 0113198 A1	22-02-2001
		WO 0113199 A1	22-02-2001
		JP 2003507784 T	25-02-2003
		JP 2003507785 T	25-02-2003
US 2003018892 A1	23-01-2003	WO 03009115 A1	30-01-2003
US 6233683 B1	15-05-2001	AT 281680 T	15-11-2004
		AU 746459 B2	02-05-2002
		AU 6578698 A	20-10-1998
		CA 2288824 A1	01-10-1998
		DE 69827405 D1	09-12-2004
		EP 1004992 A2	31-05-2000
		EP 1021801 A1	26-07-2000
		US 6005942 A	21-12-1999
		WO 9843212 A1	01-10-1998